KPMG

Modernizing Security Operations with KPMG and Google Chronicle

August 2020

Speakers

Freddie Mulyadi

Director
KPMG Siddharta Advisory

Eryk B. Pratama

Assistant Manager
KPMG Siddharta Advisory

Sandeep Patil

Regional Lead, Chronicle & Security Partnership
Google Cloud

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Agenda

- **Cyber Threats in Indonesia**
- **Common SOC Problems**
- **How Chronicle Enable a Modern SOC**

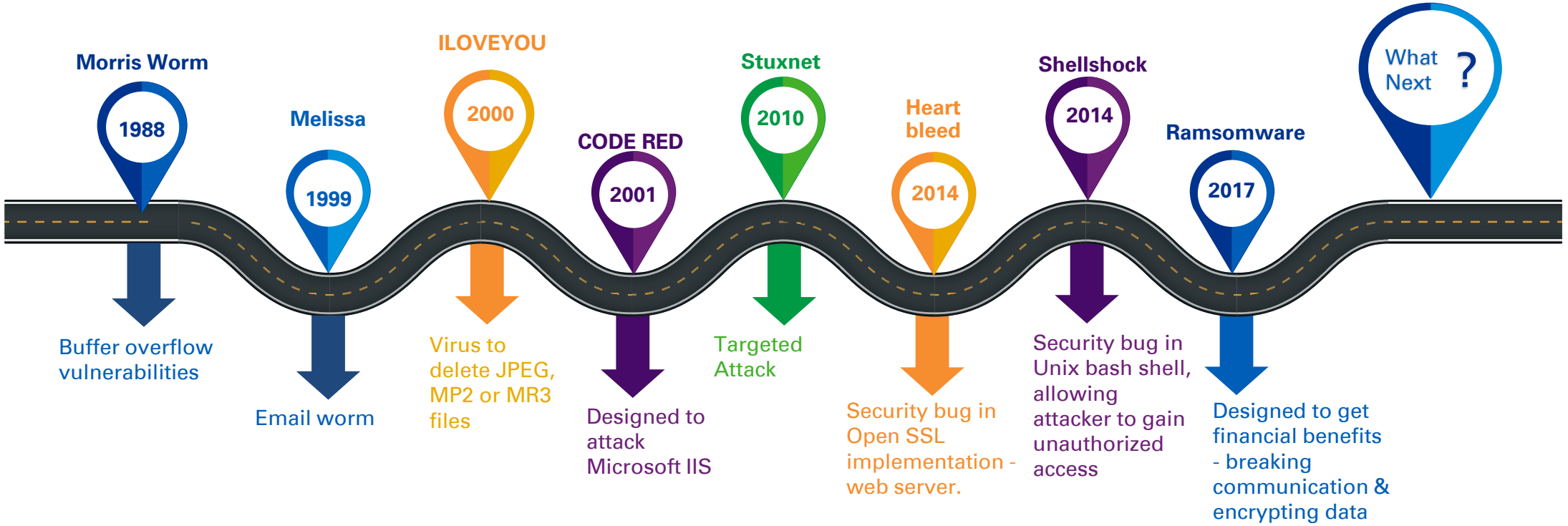
© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Evolution of Cyber Threat Pattern

Cyber is a continuous war

Stop Neglecting

Prepare before you are attacked



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

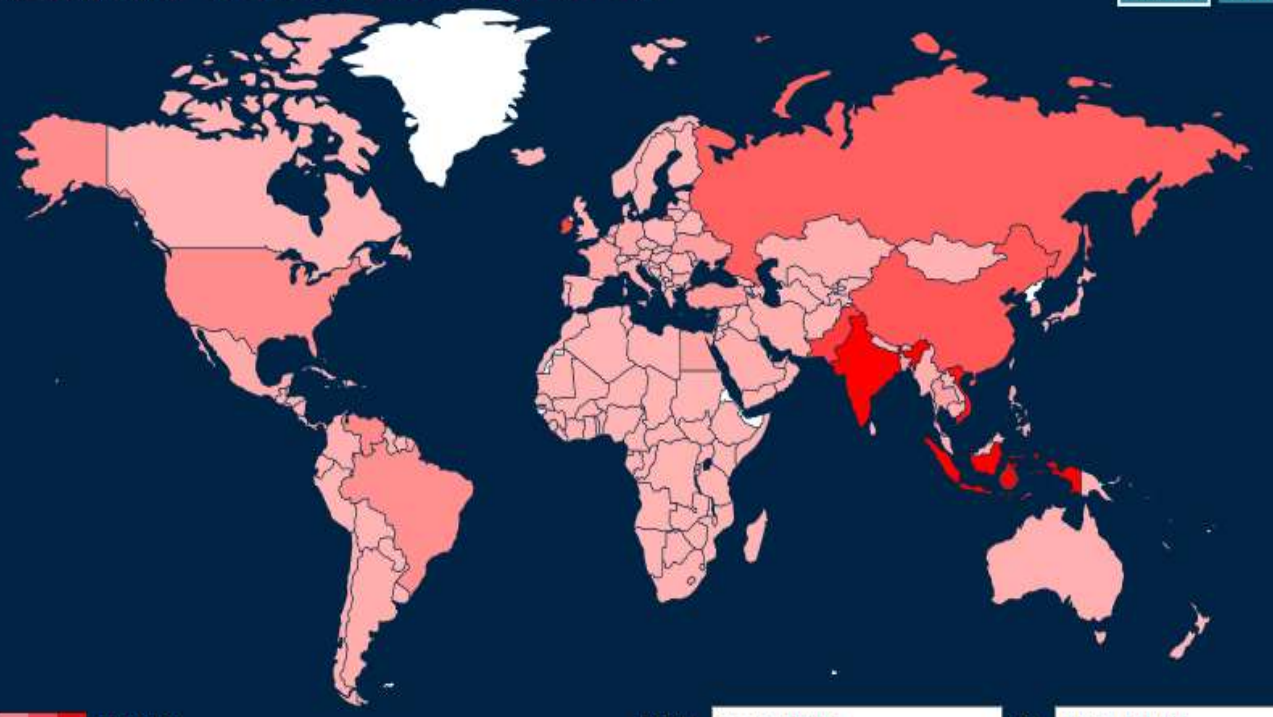
INFORMASI SERANGAN SIBER

03 AUGUST 2020

9:29:16

SUMBER SERANGAN - [2020-07-03 S/D 2020-08-03]

DUNIA | INDONESIA



0 — 4,218,782

FROM: 2020-07-03 TO: 2020-08-03

1 MONTH | 3 MONTH | 6 MONTH | 1 YEAR | YTD

PERINGKAT SERANGAN

INDONESIA	4,218,782
INDIA	3,537,750
VIETNAM	2,673,239
PAKISTAN	1,974,221
IRELAND	1,878,654

LIVE FEED

TIME	COUNTRY	PORT

TREN MALWARE

...7D9 (MALWARE/WIN32.GENERIC.C1960796)
LOW — JUMLAH SERANGAN: 15,785

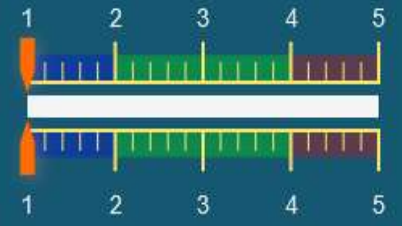
...CD8 (MALWARE/WIN32.GENERIC.C1991967)
LOW — JUMLAH SERANGAN: 3,162

...709 (TROJAN/WIN32.SWISYN.C2105126)
LOW — JUMLAH SERANGAN: 1,327

...562 (MALWARE/WIN32.GENERIC.C1991967)
LOW — JUMLAH SERANGAN: 400

...5A2 (TROJAN/WIN32.SWISYN.C2105126)
LOW — JUMLAH SERANGAN: 365

Risk Low

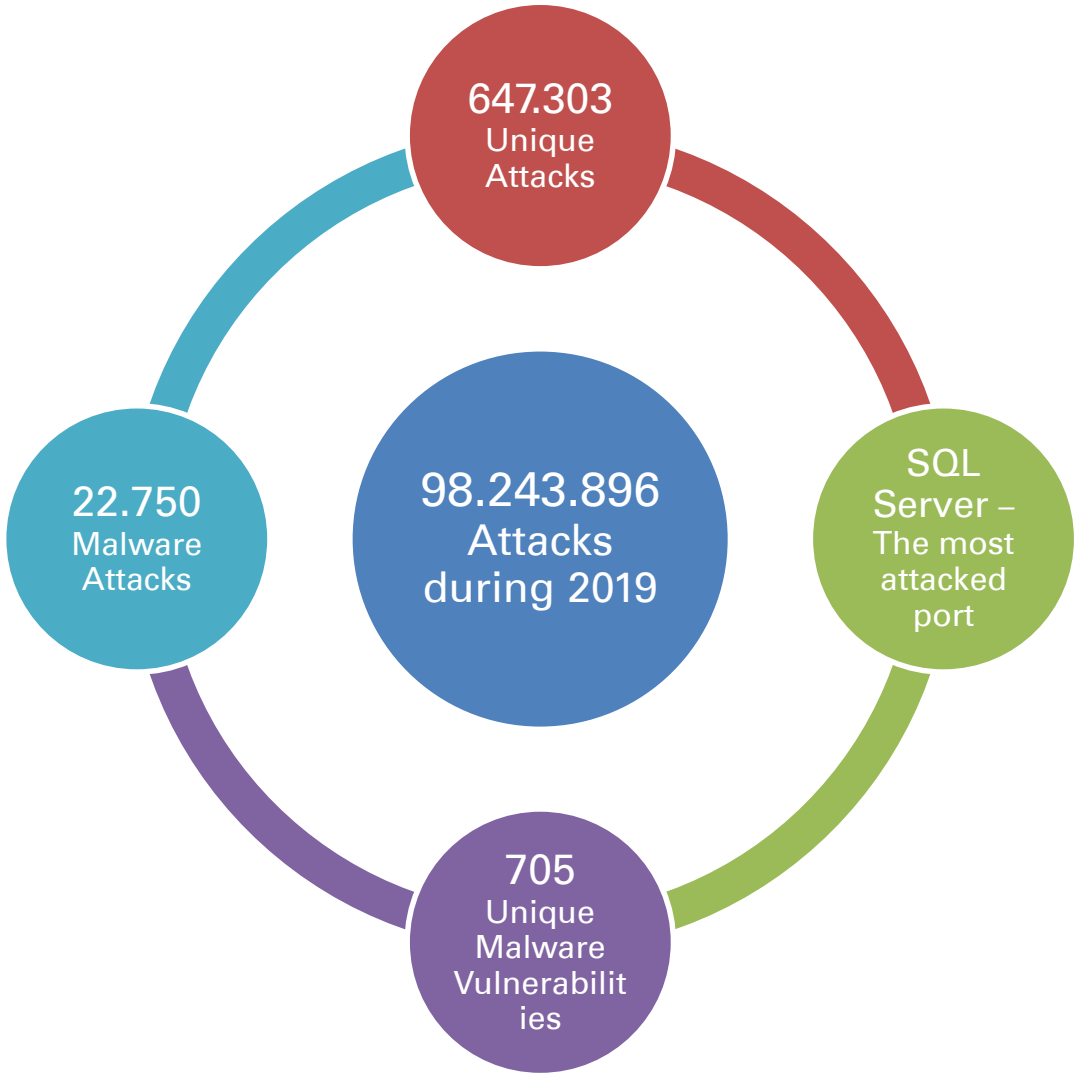


VIRTUAL ASSISTANT

Indonesia Honeynet Project

Popular Cyber Threats in Indonesia - 2019

- Over 98M Attacks in 2019
- Malware –Trojan, Viruses, Ransomware, etc
- Source and target of attacks
- India, Indonesia, Vietnam, China, and USA become the top attack sources
- Over 22.750 malware attakcs



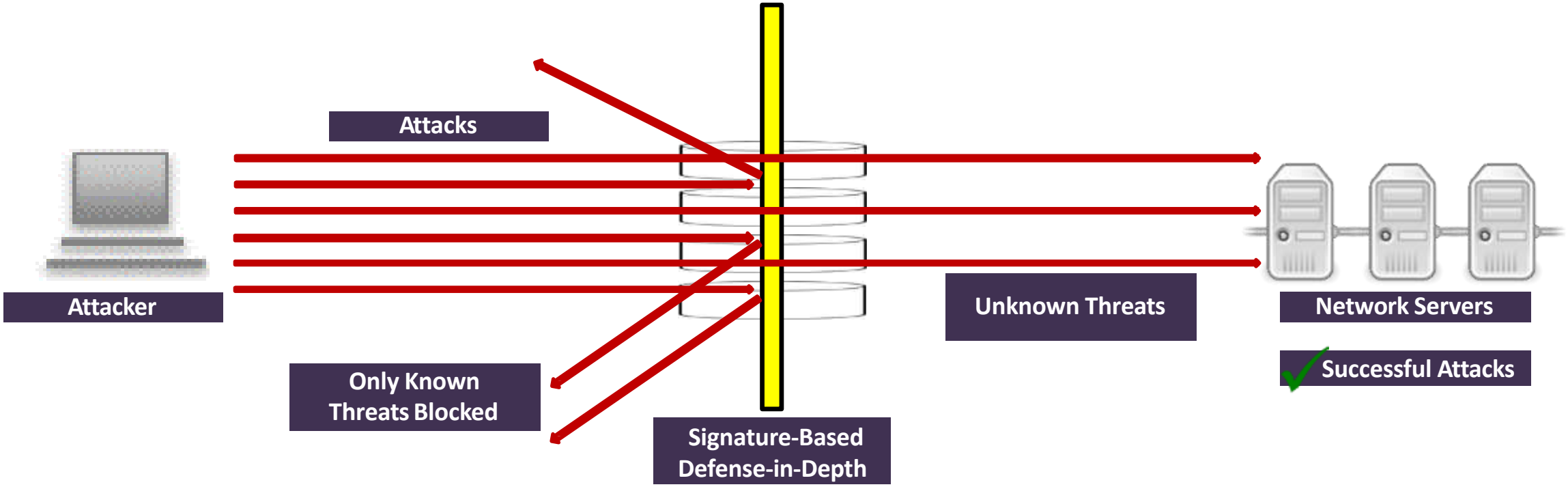
Source: BSSN – Laporan Tahunan Honeynet Project 2019

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Security Operations

Security Operations | Signature-Based Defenses

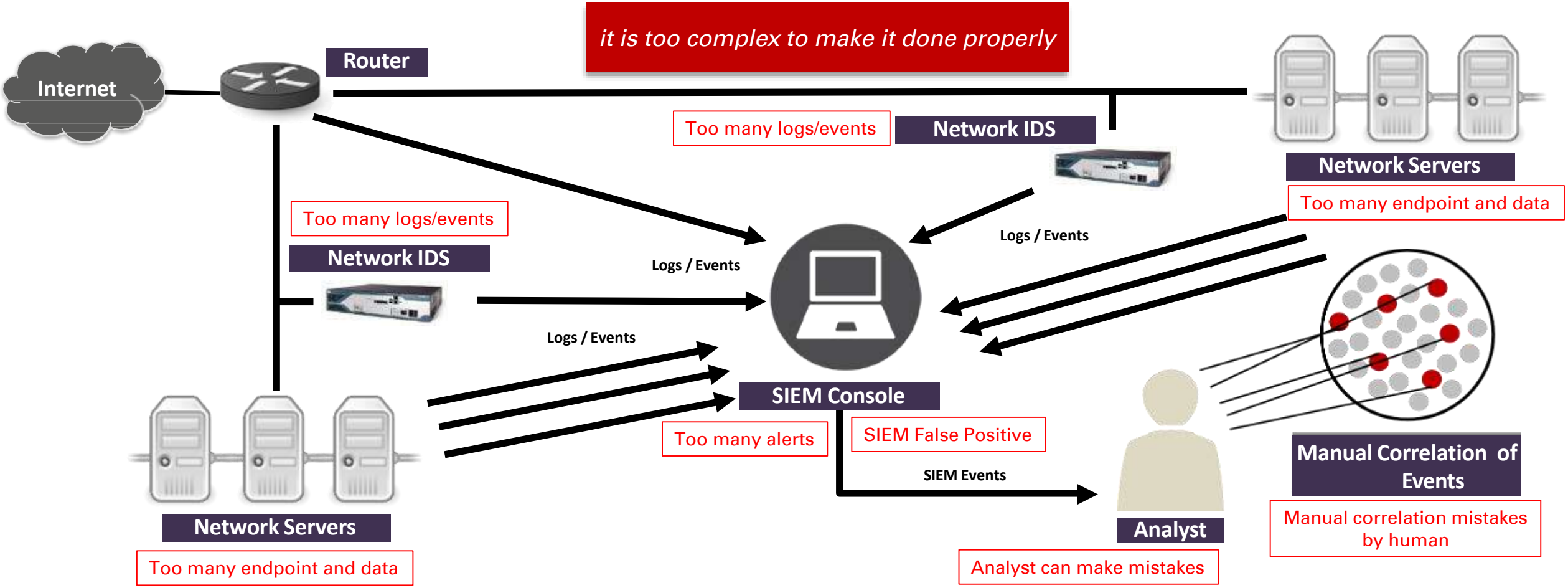
Historically, security operations has been concerned with mass attacks. These attacks were defended against by performing analysis on the first instances discovered, followed by attempting to quickly disseminate signatures and indicators of compromise (IOCs) into security controls. A few of the initial victims suffer, but everyone else could detect and block the attacks. These attacks merely generated "noise" on the network and provided no contextual information to security analysts.



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Security Operations | Common SOC Battle Rhythm

Common organization defends against network attacks reactively via a Monitor and Respond strategy. Security controls passively gather network traffic data and feed non-contextual information on multiple potential threats to the SIEM. The SIEM then issues numerous alerts that merely generate noise and do not enable security analysts to quickly correlate log data.



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

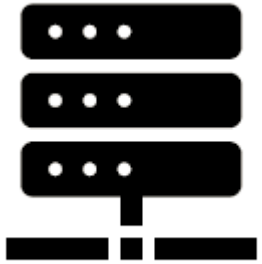
The Six Principal SOC Problems

SOC fails silently – how do you know it work?

Too many false positive

Lots of manual labor to make sense

Technology is too slow



Too much data to process

No quick enough to act

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Solve Security Data Overload

People really don't want SIEM. They want something better and security analytics is where everyone is trying to go. Security Analytics includes better SIEM but also threat intelligence, user and identity management, vulnerability management, and other key capabilities.

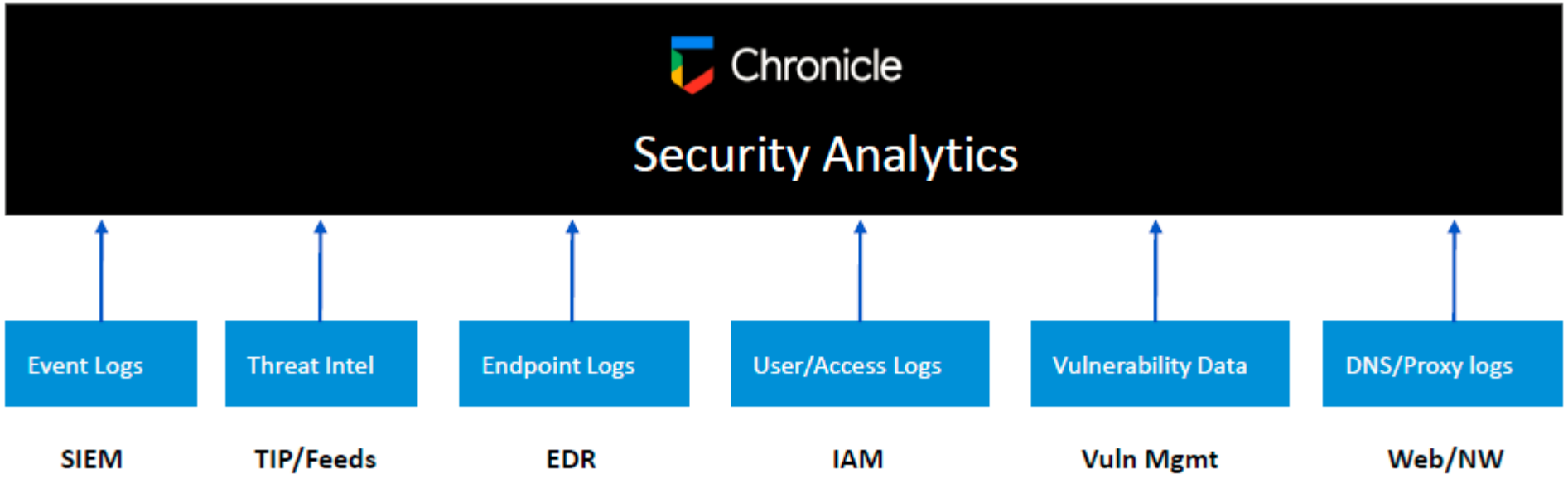
SIEM Challenges	NextGen Security Analytics
Can't scale Legacy platforms were not built for petabyte scale	**Cloud-native:** Operate at Cloud scale and speed
Too expensive Ingestion based pricing forces customers to limit what is collected and retained	**Fixed Cost:** No penalty for analyzing everything
Misses threats Incomplete data, Teams unable to see relationships between malicious indicators and events across time	**Clear Signals:** Curated intel X enriched telemetry X YARA

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Google Chronicle

Security Analytics: Detect, Hunt, Respond

Chronicle's mission is to build a planet-scale system for storing and analyzing all enterprise security telemetry and making it useful for detecting, hunting, and responding to current and emerging threats. We make the platform intelligent by integrating customers' data with unique global threat signals that only Google has.



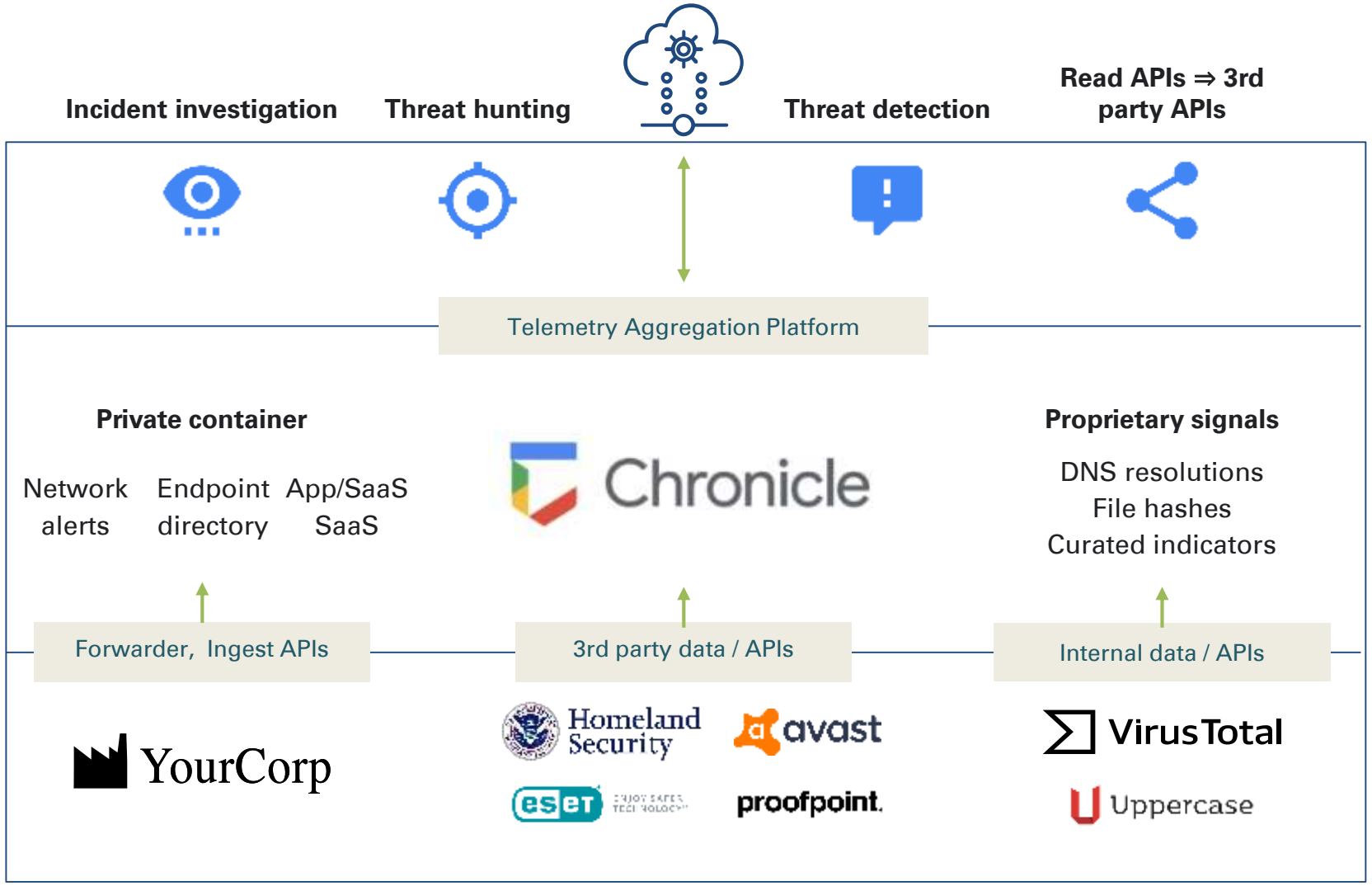
© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Chronicle Architecture

Specialized applications for investigation

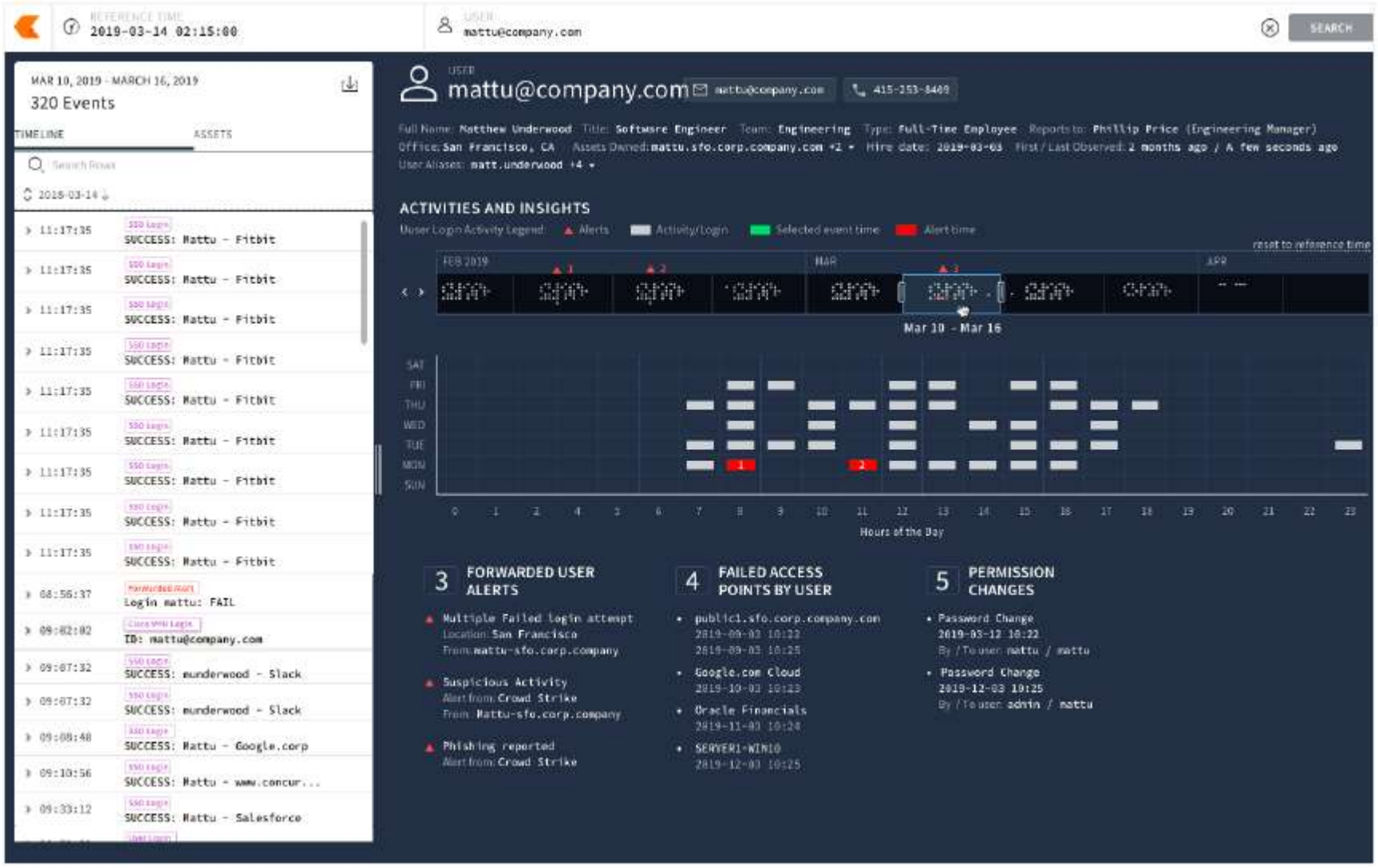
Retain, analyze, and automate

Fed with enterprise telemetry, 3rd party threat feeds, and curated threat signals



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Example: User View



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

What Makes Chronicle Different

Intelligent data fusion

Timelines and enriched data model for investigation and detection

Continuous IoC Matching

Continuous, retrospective analysis of telemetry vs. threat intelligence

Modern threat detection

YARA-L for detecting modern malware-based threats

Hunt at Google speed

Sub-second searches against petabytes of data

Self-managed

Unlimited scale-out without customer tuning, sizing, or management

Disruptive economics

Full security telemetry retention, analysis at a fixed, predictable cost

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Intelligent Data Fusion

Unified data model

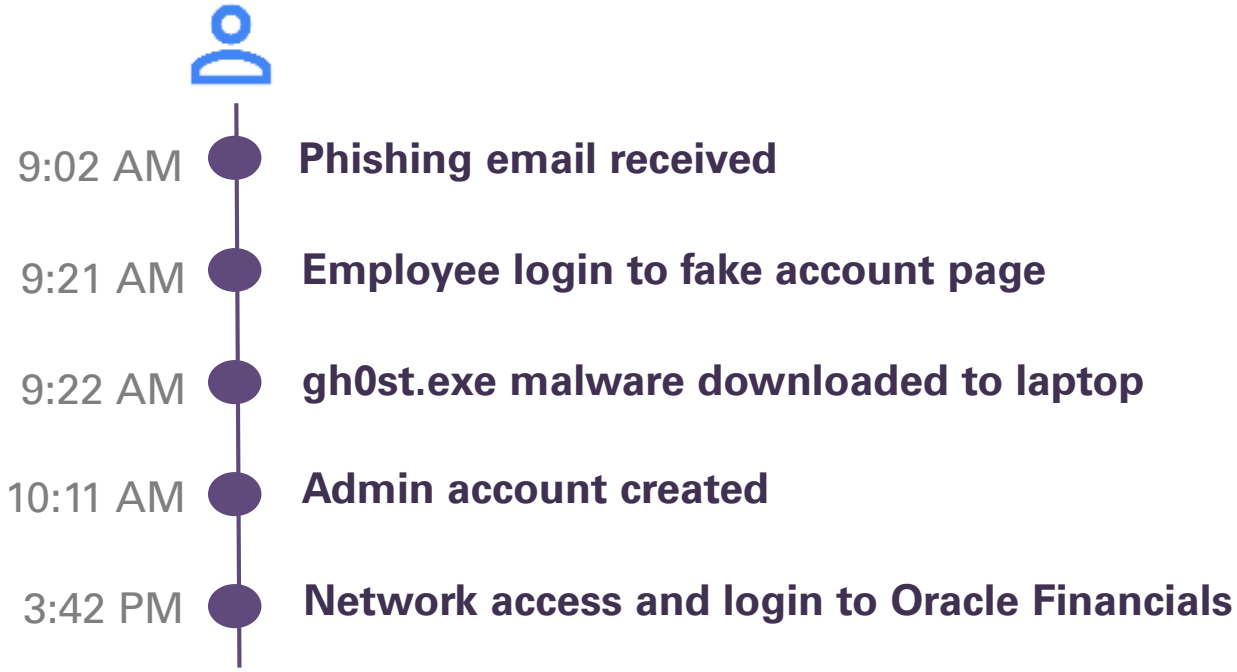
Rich, extensible data model spanning Asset, User and IoC dimensions and attributes

IP to host correlation

Automated IP to host correlation enables instant asset and IoC analytics

Canonical event deduplication

Logical event layer (user logins, network connections etc.) and visualization simplifies and expedites analysis



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Continuous IoC Evaluation

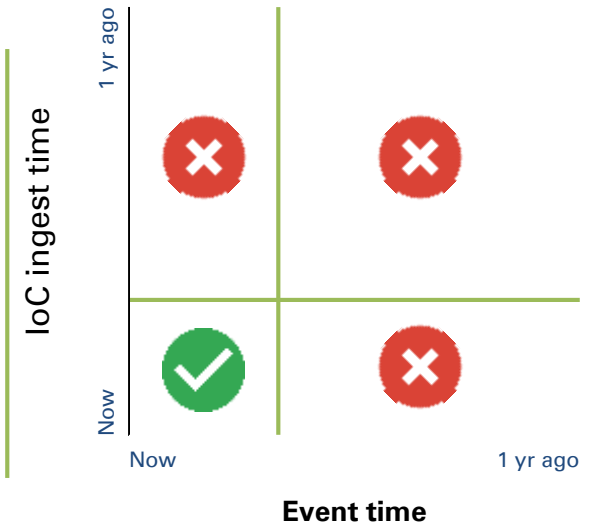
Automated, continuous, retroactive IoC matching

Instant correlation of IoCs against 1 full year of security telemetry

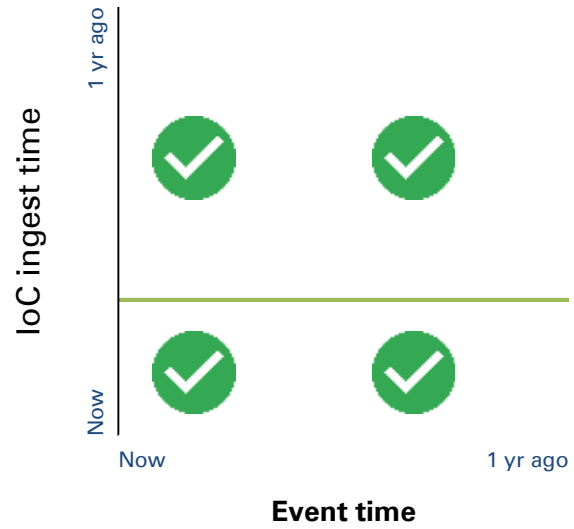
Out of the box intelligence feeds for IPs, domains, URLs, and files

Support for customer owned threat intelligence subscriptions and Threat Intel Platforms (TIPs)

Legacy SIEM tools



Chronicle



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Disruptive Economics

Future proof investment

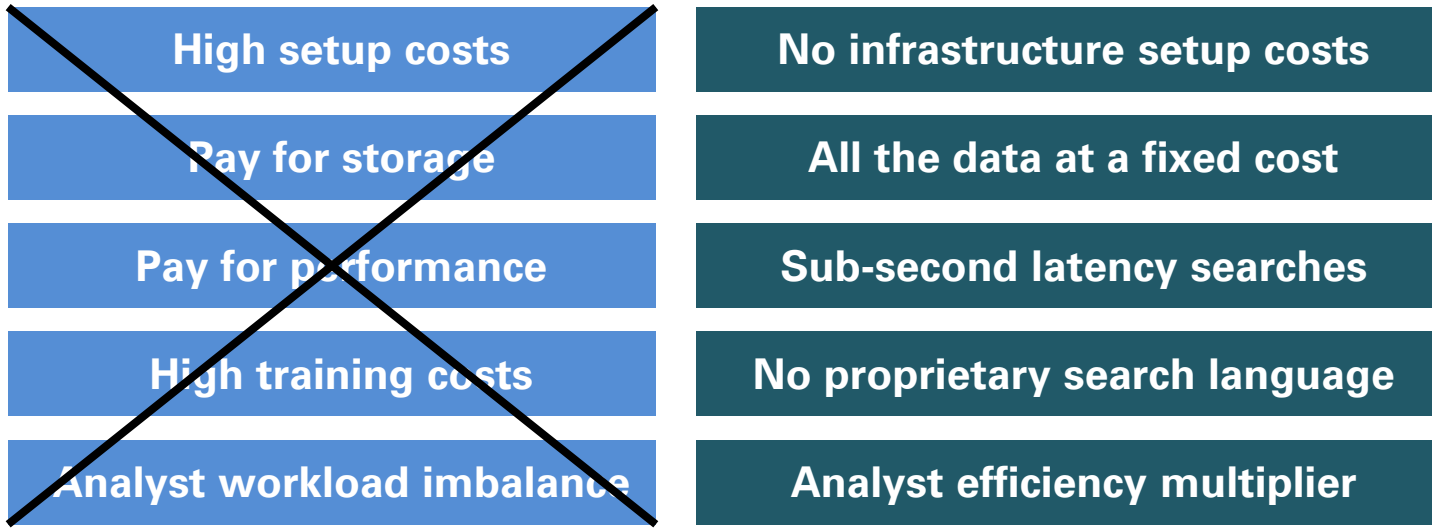
Capture, analyze all enterprise security telemetry at a fixed, predictable cost

Eliminate capex costs

SaaS model eliminates setup and expansion capex

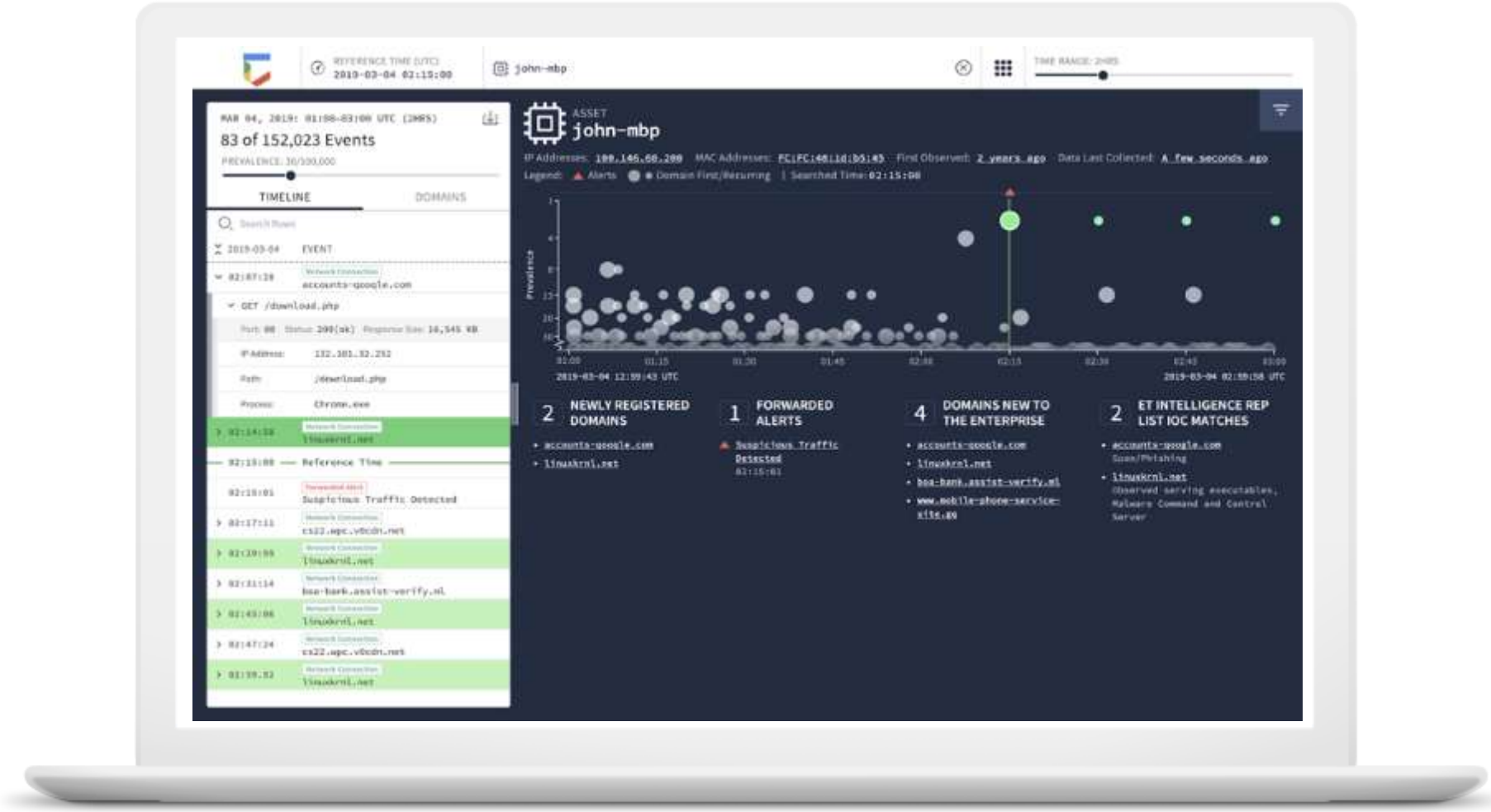
Balance SOC workload

Contextually relevant insights enable faster incident investigation and resolution



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Demo



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Sending your telemetry to Chronicle

Install Chronicle Forwarder

Flexible and able to forward telemetry from existing systems like Splunk, Syslog, or Packet Capture

Telemetry sent securely to cloud

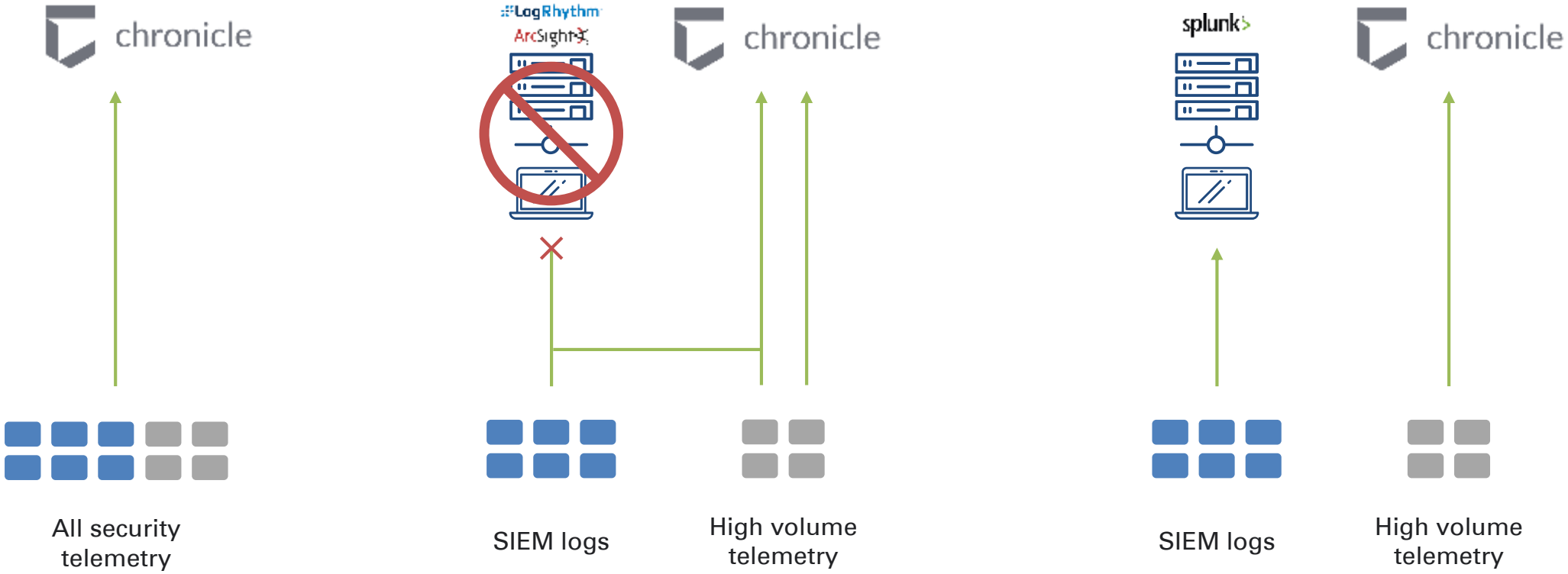
Telemetry sent via gRPC, encrypted in transit, at rest

GUI access via SSO

SAML-based authentication (support for the Okta, Ping, Duo, and others)

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Deployment options



© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Supported Data Sources (as per May 2020) - Summary

Example – Partial list

Advanced Threat Protection
- Microsoft Defender ATP

Alerts
- AlphaSOC
- Carbon Black Defense
- Cisco ASA
- Crowdstrike
- FireEye
- Microsoft Advanced Threat Analytics
- Netskope
- Palo Alto Networks
- Snort
- Suricata
- Zscaler

Antivirus
- Bitdefender
- Cisco AMP
- Cylance
- Sophos
- Trend Micro

Application
- Microsoft Office 365

Authentication
- Aruba ClearPass
- Azure AD
- Centrify
- Cisco Access Control Server (ACS)
- Cisco ISE
- Duo
- OKTA
- RSA Authentication Manager version 8.1

Cloud
- AWS Virtual Private Cloud (VPC) Flow
- GCP Virtual Private Cloud (VPC)

PAM
- CyberArk

Endpoint
- McAfee ePolicy Orchestrator

EDR
- Carbon Black Defense
- Carbon Black Response
- Check Point SandBlast
- Cisco AMP
- Crowd Strike
- Digital Guardian
- ESET
- LimaCharlie
- McAfee Endpoint Security
- Microsod

WAF
- Citrix Netscaler
- Imperva WAF

Notes:
Any data sources can be ingested in a very simple way

IOC
- Anomali
- Crowd Strike
- Department of Homland Security (DHS)
- Emerging Threats Pro
- ESET
- Proofpoint ET Pro
- Recorded Future
- OSINT

Log Aggregation/SIEM
- McAfee ESM
- Wazuh

Firewall
- Bro CONN (JSON)
- Check Point (syslog)
- Cisco ASA
- Cisco Firepower
- Fortinet
- Juniper Networks SRX
- Palo Alto Networks
- SonicWall
- Zscaler

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Q&A

Contact Us

Benson Tran
Head of IT Assurance and Cybersecurity

Wisma GKBI 35 Floor
Jl Jendral Sudirman Kav 28
Jakarta 10210 Indonesia

Phone +62 21 5740 877
Benson.Tran@kpmg.co.id

Freddie Mulyadi
Director of IT Assurance and Cybersecurity

Wisma GKBI 35 Floor
Jl Jendral Sudirman Kav 28
Jakarta 10210 Indonesia

Phone +62 21 5740 877
Freddie.Mulyadi@kpmg.co.id

Dhirendra Kumar
Director of Cybersecurity

Wisma GKBI 35 Floor
Jl Jendral Sudirman Kav 28
Jakarta 10210 Indonesia

Phone +62 21 5740 877
Dhirendra.kumar@kpmg.co.id

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG Siddharta Advisory, an Indonesian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.